双符号形式による楕円曲線暗号系 (計算理論とアルゴリズムの新展開)

AUTHOR(S):

丁, 峰; 神保, 秀司; 橋口, 攻三郎

数理解析研究所講究録
1489巻 2006年 167-173

双符号形式による楕円曲線暗号系

丁 峰　神保 秀司　橋口 攻三郎　　岡山大学 大学院 自然科学研究科
Feng Ding, Shuji Jimbo, Kosaburo Hashiguchi
Graduate School of Natural Science and Technology, Okayama University

1 序論

符号理論は2つの部分, 即ち, 単チャンネル符号理論と多チャンネル符号理論に区分される. 単チャンネル符号は, ブロック符号, 変長符号, 誤り訂正符号などのようなたくさんの族について研究された. 単チャンネル符号理論はとても深いし, 大きいし, 実用的かつ, 理論的であり, 代数学, 組合せ論とコンピュータ科学のたくさんの分枝と関連している. 特に, 形式言語理論の分枝としてとても深く発展してきた. その一方, 多チャンネル符号理論は一般にエントロピー, 伝送速度, 雑音, チャンネル容量, 歪曲速度などのような情報理論の概念と関係している. もし代数学, 形式言語理論と組合せ論を関係づける多チャンネル符号理論を発展すれば, これはとても面白い. 我々の研究の意図はそのような理論を発展させることである.

この論文の中に, 我々は双符号と呼ばれる符号の新しい族を紹介する. Σ とは空集合でない有限アルファベットである. Σ^* とは Σ により生成される自由単位半群である. 双符号とは, 任意の $p,q \geq 1, 1 \leq i_1, i_2, \ldots, i_p, j_1, j_2, \ldots, j_q \leq n$ に対して, $x_{i_1}x_{i_2}\ldots x_{i_p}y_{i_p}\ldots y_{i_1} = x_{j_1}x_{j_2}\ldots x_{j_q}y_{j_q}\ldots y_{j_1}$ ならば, 全ての $1 \leq k \leq p$ に対して, $p = q$ かつ $i_k = j_k$ が成り立つような語の対の有限系列 $Z = ((x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n))(n \geq 1, x_i, y_i \in \Sigma^*)$ である. 任意の双符号 Z は2チャンネル符号としても1チャンネル符号としても用いることができる。双符号理論は1チャンネルと2チャンネル符号理論, 誤り訂正符号理論, 暗号と形式語言理論に関連して発展することが期待される. 我々の研究室において双符号形式に基づいたRSA暗号系の族がいくつか提案されている. EIGamalは離散対数問題に基づいた公開鍵暗号系を提案した. この暗号系はEIGamal暗号系と呼ばれる. 楕円曲線暗号系はEIGamal暗号系を離散楕円曲線上で実現した暗号系である. 本論文において双符号形式に基づいた楕円曲線暗号系を提案する. ([2] において、8つの暗号系が提案されている。) 双符号は情報を分散して表現できるので, 暗号系の表現に有効であると考えられる.

2 双符号

Σ とは空集合でない有限アルファベット (記号の集合) である. Σ^* とは Σ により生成される自由単位半群である. Σ^* 上の要素 $w = a_1 \ldots a_n (n \geq 0, a_i \in \Sigma)$ は (Σ 上の) 語である. 長さ0の語は空語と呼ばれ λ で表す. Σ^+ は空でない語 (Σ 上の) の集合である. 任意の $x, y, z \in \Sigma^*$ に対し x は xy の接頭語で, z は yz の接尾語であり, y は xyz の因子である. 空集合は ϕ で表される. 本論

文では, (1 チャンネル) 符号は有限符号を表す. 通常, 符号は (符号) 語の有限集合 $\{x_1,\ldots,x_n\}$ により表される. しかしながら表記の便宜上, 本論文では以下の定義を使用する.

定義 2.1

$seq(\Sigma^*)$ は Σ 上の有限長である (空でない) 語系列の集合とする. 任意の $X=(x_1,\ldots,x_n)\in seq(\Sigma^*)$ に関し, $n\geq 1$ とすべての $1\leq i\leq n$ に対し $x_i\in\Sigma^*$ を満たす. n は X の長さで $|X|$ で表される.

定義 2.2

符号は有限長の (空でない) 語系列, $X=(x_1,\ldots,x_n)\in seq(\Sigma^*)$ である. つまり任意の $p,q\geq 1$ かつ $i_1,\ldots,i_p,j_1,\ldots,j_q(1\leq i_k,j_l\leq n)$ に対し, $x_{i_1}\ldots x_{i_p}=x_{j_1}\ldots x_{j_q}$ なら, $p=q$ かつすべての $1\leq k\leq p$ に対し $i_k=j_k$ が成り立つ. この時各 x_i は (X の) 符号語と呼ばれる.

次の定理はよく知られている.

定理 2.1

任意の与えられた語の有限語列, $X=(x_1,\ldots,x_n)\in seq(\Sigma^*)$ に対し, X が符号か決定できるアルゴリズムが存在する.

定義 2.3

$seq(\Sigma^*\times\Sigma^*)$ は Σ 上の語の対の有限 (空でない) 系列の集合とする.

任意の $Z=((x_1,y_1),\ldots,(x_n,y_n))\in seq(\Sigma^*\times\Sigma^*)$ に対し, $n\geq 1$ かつ任意の $1\leq i\leq n$ に対し $x_i,y_i\in\Sigma^*$ である. n は Z の長さであり, $|Z|$ で表すものとする.

定義 2.4

任意の $Z=((x_1,y_1),\ldots,(x_n,y_n))\in seq(\Sigma^*\times\Sigma^*)$ に対し, $Z^{(+)}$ は語の集合
$\{x_{i_1}\ldots x_{i_p}y_{i_p}\ldots y_{i_1}|\forall k,1\leq k\leq p,p\geq 1$ かつ $1\leq i_k\leq n\}$ を意味する.

次の命題は, 形式言語理論においてよく知られている.

命題 2.1

任意の $Z\in seq(\Sigma^*\times\Sigma^*)$ に対し, $Z^{(+)}$ は線形文脈自由言語である.

例 2.1

$\Sigma=\{a,b,c\}$, $Z_1=((ab,a),(c,a),(a,a),(bc,a))$ かつ $Z_2=((a,a),(ab,a),(abc,a))$ とする. ここで, Z_1 は双符号でない. なぜなら $abcaa\equiv(ab,c,a,a)\equiv(a,bc,a,a)$ であるためである. しかし Z_2 は容易にわかるように双符号である.

定義 2.5

任意の有限語順序対列 $Z=((x_1,y_1),\ldots,(x_n,y_n))\in seq(\Sigma^*\times\Sigma^*)$ が与えられたとき, Z が双符号であるかどうかを決定する問題を双符号判定問題と呼ぶ.

定理 2.2

双符号判定問題は非可解である.

この定理は, Post 対応問題を双符号判定問題に帰着させることより証明できる.

3 楕円曲線暗号系

楕円曲線はある種の2変数方程式の解の集合により記述される．素数 p に対して modulo p により定義される楕円曲線は公開鍵暗号系において中心的重要性を持つ．自然数 n に対して，Z_n, Z_n^* を次のように置く．

$$Z_n = \{0, 1, 2, \ldots, n-1\}$$

$$Z_n^* = \{n \text{ とは互いに素な, 法 } n \text{ での剰余の集合 }\}$$

$p > 3$ は素数とする．$\mathbb{Z}_p$ 上の楕円曲線は実数上の楕円曲線と同じように,(加法演算も同様に) 定義される．すべての実数上の演算が，$\mathbb{Z}_p$ 上における類似の演算により置換される．

定義 3.1

$p > 3$ は素数とする．$\mathbb{Z}_p$ 上の楕円曲線 $y^2 = x^3 + ax + b$ は合同関係式

$$y^2 \equiv x^3 + ax + b \pmod{p} \tag{3.1}$$

に対する解 $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ の集合である．ここで，$a, b \in \mathbb{Z}_p$ は $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ を満たす定数である，また，特殊点 $\mathcal{O}$ は無限遠点と称される．これらの要素の集合は E によって定義される．

E 上の加法演算は次のように定義される (ここで，すべての算術演算は $\mathbb{Z}_p$ において行われる)：

$$P = (x_1, y_1)$$

かつ

$$Q = (x_2, y_2)$$

は E 上の点であると仮定する．$x_2 = x_1$ かつ $y_2 = -y_1$ であれば，$P + Q = \mathcal{O}$ である; さもなければ，$P + Q = (x_3, y_3)$ である．ここで，

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

かつ

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & P \neq Q \text{ のとき} \\ (3x_1^2 + a)(2y_1)^{-1} & P = Q \text{ のとき} \end{cases}$$

最後に，すべての $P \in E$ に対して，

$$P + \mathcal{O} = \mathcal{O} + P = P$$

と定義する．

$\mathbb{Z}_p$ 上の楕円曲線上の点の加法は実数上の楕円曲線のような，良い幾何学的説明を持ってないことに注意する．しかし，同様な式は加法を定義することに利用され，その結果，対 $(E, +)$ は可換群を形成する．

楕円曲線上で ElGamal 暗号系を実行することに関して，いくらかの難しさはある．より効率のよい ElGamal-型系は，いわゆる *ECIES*(*Elliptic Curve Integrated Encryption Scheme*) であ

る．$ECIES$ は相当に複雑な記述をもち，これは対称鍵暗号化と通信認証符号に対応する．我々は簡約系について述べる．これは基本的に，$ECIES$ で使用される楕円曲線に基づいた ElGamal 公開鍵暗号化体系である．

楕円曲線上の点の記憶容量を減じる点圧縮と呼ばれる標準的操作も使用する．楕円曲線 E 上の (非無限) 点は対 (x,y) である，ここで，$y^2 \equiv x^3+ax+b \pmod p$ である．既知の x の値に対し，y は 2 個の可能な値がある ($x^3+ax+b \equiv 0 \pmod p$ でない限り)．2 個の可能な y 値は互いに法 p の下で負の数となる．p は奇数であるから，y の 2 個の可能な値の一方は偶数であり，他方は奇数である．x の値と各々のビット $y \bmod 2$ によって，E 上の唯一の点 $P=(x,y)$ を決定することできる．

点圧縮の演算は次の関数のように表せる

$$\text{POINTCOMPRESS} : E\backslash\{\mathcal{O}\} \to \mathbb{Z}_p \times \mathbb{Z}_2$$

これは以下のように定義される:

$$POINTCOMPRESS(P) = (x, y \bmod 2)$$

ここで，$P=(x,y) \in E$ である．以下の暗号系において，x は 2 進系列で表わされる．このため，$(x, y \bmod 2)$ を xa で表わす．ここで，$a = y \bmod 2 (\in \{0,1\})$ である．

簡約化 $ECIES$ と呼ばれる暗号系は暗号系 3.1 のように表わされる．

暗号系 3.1

簡約化　$ECIES$

E は $\mathbb{Z}_p (p>3$ は素数である) 上で定義される楕円曲線であり，E は離散対数問題を解くこと $(1 \le k \le n-1)$ が困難な素位数 n の巡回部分群 $H = < P >$ を持っているとする．ここで，$P \in E$ であり，$< P >= \{\mathcal{O}, P, 2P, \ldots, (n-1)P\}$ である．また，$\beta \in < P > -\{\mathcal{O}\}$ が与えられたとき，$\beta = hP$ である，h を求めることが困難である．

$\mathcal{P} = \mathbb{Z}_p^*$ かつ $\mathcal{C} = (\mathbb{Z}_p \times \mathbb{Z}_2) \times \mathbb{Z}_p^*$ として，鍵の集合を

$$\mathcal{K} = \{(E, P, m, Q, n) : Q = mP\}$$

とする．

値 P, Q と n は公開鍵であり，$m \in \mathbb{Z}_n^*$ は秘密鍵である．

$K = (E, P, m, Q, n)$ と (秘密の) 任意の乱数 $k \in \mathbb{Z}_n^*$ と平文 $x \in \mathbb{Z}_p^*$ に対して，暗号鍵 e_K を用いて，

$$e_K(x,k) = (POINTCOMPRESS(kP), xx_0 \bmod p) (= (y_1, y_2))$$

を求める．ここで，$kQ = (x_0, y_0)$ かつ $x_0 \neq 0$ である．

暗号文 $y = (y_1, y_2) (= e_K(x,k))$ (ここで，$y_1 \in \mathbb{Z}_p \times \mathbb{Z}_2$ かつ $y_2 \in \mathbb{Z}_p^*$) に対して，復号鍵 d_K を用いて，

$$d_K(y) = y_2 (x_0)^{-1} \bmod p$$

を求める．ここで，$(x_0, y_0) = mPOINTDECOMPRESS(y_1)$ であり，$d_K(y) = x$ である．

4 双符号を用いた楕円曲線公開鍵暗号系の提案

この章では, 双符号を用いた楕円曲線公開鍵暗号系を 1 個提案する. (文献 [2] において, 8 個の暗号系が提案されている).

公開鍵暗号系 1 では, 鍵を 4 セット使用し, 1, 2 セット目で暗号化した平文を双符号ブロックとして分割するための長さ l_1, l_2 を, 3 セット目で γ(ここで, γ は 4.1.1 で示すようにランダムに構成するある 2 進系列である) をブロックとして分割するための長さ l_3 を, 4 セット目で平文の暗号化と復号化を行う. よって, 使用する鍵の数は通常の楕円曲線公開鍵暗号系の 4 倍となる.

ここで, 実際通信されるデータは, 上述の長さ l_1, 長さ l_2 と γ を暗号化したものと, 双符号により暗号化された通信文より成る.

公開鍵暗号系 1 は次の項目により成立する.

(1) $x(\geq 2)$ の人, $A_1, \ldots, A_x$ の作る集合.

(2) 各 $1 \leq i \leq x$ に対し, A_i は簡約化 ECIES の 4 つのユニット $(p_{ij}, E_{ij}, P_{ij}, m_{ij}, Q_{ij}, n_{ij}, e_{ij}, d_{ij})$ $(j = 1,2,3,4)$ を持つ. 但し, $1 \leq i < j \leq x$ に対し, A_i と A_j のこれらのユニットは互いに異なるものとする.

(3) ここで, 全ての $1 \leq i \leq x$ に対し, 各 A_i は (P_{ij}, n_{ij}, Q_{ij}) $(j = 1,2,3,4)$ を公開する.

(4) ある平文 M を A_i に送る場合, 下記の暗号化復号化法 1 を用いて暗号文 C を送信する.

(5) 送信文を受信した A_i は, 暗号文 C に暗号化復号化法 1 を用いることにより平文 M を得る.

以下に, 暗号化復号化法 1 について形式的に記す.

4.0.1 暗号化復号化法 1

簡約化 ECIES の 4 つのユニット $(p_i, E_i, P_i, m_i, Q_i, n_i, e_i, d_i)$ $(i = 1,2,3,4)$ を持つ.

アルファベット $\Sigma = \{0,1\}$ 上のブロック符号 $U = (u_1, \ldots, u_m)$ に対して, 暗号化復号化を次のように行う. ここで, $u_i \in \Sigma^+$, $|u_i| = \lceil \log_2 p_4 \rceil$ $(1 \leq i \leq m)$ が成立しているとする.

(1) まず $1 \leq l_1 \leq \min\{\lceil \log_2 p_1 \rceil - 1, \lceil \log_2 p_2 \rceil - 1, \lceil \log_2 p_3 \rceil - 1, \lceil \log_2 p_4 \rceil - 1\}$ である正整数 l_1 を送信者が選ぶ.

(2) 送信者はランダムに $k_1 \in \mathbb{Z}_{n_1}^*$ を選ぶ. 鍵 e_1 を用いて, $e_1(l_1, k_1) = (l_{11}, l_{12})$ を求める. ここで, l_{11} と l_{12} は 2 進系列であり, $|l_{12}| = \lceil \log_2 p_1 \rceil$ である. l_{11} は POINTCOMPRESS の説明のときに述べたように, POINTCOMPRESS$(k_1 P_1) = (x', y \bmod 2)$ のとき, $l_{11} = x'a$ $(a = y \bmod 2 \in \{0,1\})$ であり, 従って, $|l_{11}| = \lceil \log_2 p_1 \rceil + 1$ である. ここで, $l_{11} = x_{011}y_{011}$, $l_{12} = x_{012}y_{012}$ とおく. ただし, $x_{011} = hp(l_{11})$, $x_{012} = hp(l_{12})$, $y_{011} = hs(l_{11})$, $y_{012} = hs(l_{12})$ とする.

(3) 次に $1 \leq l_2 \leq \min\{\lceil \log_2 p_1 \rceil - 1, \lceil \log_2 p_2 \rceil - 1, \lceil \log_2 p_3 \rceil - 1, \lceil \log_2 p_4 \rceil - 1\}$ である正整数 l_2 を送信者が選ぶ.

(4) 送信者はランダムに $k_2 \in \mathbb{Z}_{n_2}^*$ を選ぶ. 鍵 e_2 を用いて, $e_2(l_2, k_2) = (l_{21}, l_{22})$ を求める. ここで, l_{21} と l_{22} は2進系列であり, $|l_{22}| = \lceil \log_2 p_2 \rceil$ である. l_{21} はPOINTCOMPRESSの説明のときに述べたように, POINTCOMPRESS$(k_2 P_2) = (x', y \bmod 2)$ のとき, $l_{21} = x'a$ $(a = y \bmod 2 \in \{0,1\})$ であり, 従って, $|l_{21}| = \lceil \log_2 p_2 \rceil + 1$ である. ここで, $l_{21} = x_{021}y_{021}$, $l_{22} = x_{022}y_{022}$ とおく. ただし, $|x_{021}| = |x_{022}| = l_1$, $|y_{021}| = \lceil \log_2 p_2 \rceil + 1 - l_1$ かつ $|y_{022}| = \lceil \log_2 p_2 \rceil - l_1$ とする.

(5) 送信者が通信文 $u_{i_1}u_{i_2}\cdots u_{i_t} (t \geq 1, 1 \leq i_j \leq m)$ を送信したいとする.

(6) 送信者は長さ t の2進系列 $\gamma = a_1 \cdots a_t$ をランダムに生成する. ここで, $a_i \in \{0,1\} (1 \leq i \leq t)$ である.

(7) 送信者は, γ を長さ $\lceil \log_2 p_3 \rceil$ のブロックに分割する. つまり, $\gamma = b_1 b_2 \cdots b_s (1 \leq s < t)$ とする. ただし, $1 \leq i \leq s$ に対して, $b_i \in \{0,1\}^+$, $|b_i| = \lceil \log_2 p_3 \rceil$ であり, 必要なら, (6) の γ の右にいくつかの0を並べて $|\gamma| = s \times \lceil \log_2 p_3 \rceil$ となる新しい γ を作る. $0 \leq b_i < p_3 (1 \leq i \leq s)$.

(8) 送信者はランダムに $k_3 \in \mathbb{Z}_{n_3}^*$ を選ぶ. 各 $1 \leq i \leq s$ に対して, 鍵 e_3 を用いて, $e_3(b_i, k_3) = (z_{01}, l_{3i2})$ を求める. ここで, z_{01} と l_{3i2} は2進系列であり, $|l_{3i2}| = \lceil \log_2 p_3 \rceil$ である. z_{01} はPOINTCOMPRESSの説明のときに述べたように, POINTCOMPRESS$(k_3 P_3) = (x', y \bmod 2)$ のとき, $z_{01} = x'a$ $(a = y \bmod 2 \in \{0,1\})$ であり, 従って, $|z_{01}| = \lceil \log_2 p_3 \rceil + 1$ である. ここで, $z_{01} = x_{031}y_{031}$, $l_{3i2} = x_{03i2}y_{03i2}$ とおく. ただし, $|x_{031}| = |x_{03i2}| = l_2$, $|y_{031}| = \lceil \log_2 p_3 \rceil + 1 - l_2$ かつ $|y_{03i2}| = \lceil \log_2 p_3 \rceil - l_2$ とする.

(9) 送信者はランダムに $k_4 \in \mathbb{Z}_{n_4}^*$ を選ぶ. 各 $1 \leq i \leq m$ に対し, 鍵 e_4 を用いて, $e_4(u_i, k_4) = (z_0, z_i)$ を求める. ただし, z_i は長さ $\lceil \log_2 p_4 \rceil$ の2進系列とする. また z_0 はPOINTCOMPRESSの説明のときに述べたように, POINTCOMPRESS$(k_4 P_4) = (x', y \bmod 2)$ のとき, $z_0 = x'a$ $(a = y \bmod 2 \in \{0,1\})$ であり, 従って, $|z_0| = \lceil \log_2 p_4 \rceil + 1$ である.

(10) 双符号 $Z(U, l_1, l_2, \gamma)$ を次のように定義する

$$\begin{aligned} Z(U, l_1, l_2, \gamma) \;=\; & ((x_{011}, y_{011}), (x_{012}, y_{012}), (x_{021}, y_{021}), (x_{022}, y_{022}), \\ & (x_{031}, y_{031}), (x_{0312}, y_{0312}), (x_{0322}, y_{0322}), \cdots, \\ & (x_{03s2}, y_{03s2}), (x_0, y_0), (x_1, y_1), (x_2, y_2), \cdots, (x_m, y_m)) \end{aligned}$$

ここで, $z_0 = x_0 y_0$, $|x_0| = l_1$, $|y_0| = \lceil \log_2 p_4 \rceil + 1 - l_1$,
さらに, 各 $1 \leq i \leq m$ に対し, $z_i = x_i y_i$, $|x_i| = l_2$, $|y_i| = \lceil \log_2 p_4 \rceil - l_2$ である.

(11) 通信文 $u_{i_1}u_{i_2}\cdots u_{i_t}$ のかわりに次の2進系列を送信する
$x_{011}x_{012}x_{021}x_{022}x_{031}x_{0312}x_{0322}\cdots x_{03s2}x_0 X(z_{i_1})X(z_{i_2})\cdots X(z_{i_t})$
$Y(z_{i_t})Y(z_{i_{t-1}})\cdots Y(z_{i_1})y_0 y_{03s2}\cdots y_{0322}y_{0312}y_{031}y_{022}y_{021}y_{012}y_{011}$
ここで, $1 \leq j \leq t$ に対して, 次が成立する:

(a) もし $a_j = 0$ なら,
$X(z_{i_j}) = x_{i_j}$ かつ $Y(z_{i_j}) = y_{i_j}$

(b) もし $a_j = 1$ なら,
$X(z_{i_j}) = x_{i_j}^R$ かつ $Y(z_{i_j}) = y_{i_j}^R$

とする.

受信者は以下のように復号化を行う.

(1) 受信者は $x_{011}y_{011}, x_{012}y_{012}$ に対し,
鍵 d_1 を用いて, $d_1(x_{011}y_{011}, x_{012}y_{012}) = l_1$ を得る.

(2) l_1 により $z_0 = x_0y_0$ を得る.

(3) 受信者は $x_{021}y_{021}, x_{022}y_{022}$ と l_1 に対し,
鍵 d_2 を用いて, $d_2(x_{021}y_{021}, x_{022}y_{022}) = l_2$ を得る.

(4) l_2 により $X(z_{i_j})Y(z_{i_j})(1 \leq j \leq t)$ を得る.

(5) 鍵 d_3 を用いて, l_2 と $((x_{031}, y_{031}), (x_{0312}, y_{0312}), (x_{0322}, y_{0322}), \cdots, (x_{03s2}, y_{03s2}))$ より, $\gamma = a_1 \cdots a_t$ を得る.

(6) 受信者は鍵 d_4 を用いて, $X(z_{i_j})Y(z_{i_j})$ と a_j より, $d_4(z_0, z_{i_j}) = u_{i_j}$ を得る. 以上により通信文 $u_{i_1}u_{i_2}\cdots u_{i_t}$ を得る.

参考文献

[1] M.Berstel and D.Perrin, THEORY OF CODES, ACADEMIC PRESS, INC., 1985

[2] K. Hashiguchi, F. Deng and S. Jimbo, Modified simplified Curve Integrated Encryption Schemes and modified ElGamal Cryptosystems over bicodes, submitted to Theoret. Comput. Sci.

[3] K.Hashiguch, K.Hashimoto and S.Jimbo, Modified RSA cryptosystems over bicodes, Advances in Algeebra (Proceedings of ICM Satellite Conference in Algebra and Related Topics) (2002, Hong Kong), K.P.Shum, Z.X.Wan and J.P.Zhang eds, World Scientifis, 2003, pp.377-389

[4] K.Hashiguchi, T.Mizoguchi, K.Hashimoto and S.Jimbo, Bicodes and modified RSA cryptosystems, submitted to Theoret. Comput. Sci.

[5] K.Hashiguchi and T.Mizoguchi, Introduction to bicodes, Algebraic Engineering(Proceedings of The International Workshop on Formal Languages and Computer Systems, Kyoto, Japan 18-21 March 1997 and The First International Conference on Semigroups and Algebraic Engineering, Aizu, Japan 24-28 March 1997), C.L. Nehaniv and M. Ito eds, World Scientific, 1999, pp.219〜229

[6] D.R.Stinson, CRYPTGRAPHY Theory and Practice, Second Edition, CRC Press, Inc, 2002